UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/807,990	03/23/2004	Mark Maggenti		4659

23696 7590 12/15/2008
QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

EXAMINER
TRAORE, FATOUMATA

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
12/15/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com
kascanla@qualcomm.com
nanm@qualcomm.com

Office Action Summary	Application No.	Applicant(s)	
	10/807,990	MAGGENTI ET AL.	
	Examiner	Art Unit	
	FATOUMATA TRAORE	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 September 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28,33 and 34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28, 33, 34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This in response the amendment filed 09/09/2008. Claims 29-32 have been cancelled. Claims 1-28, 33 and 34 are pending and have been considered below.

Claim Rejections - 35 USC § 101

.

2. The 101 rejection to claims 7-9 and 21-24 has been withdrawn in light of applicant arguments

Response to Arguments

3. Applicant's arguments filed 09/25/2008 have been fully considered but they are not persuasive.

4. Applicant argues, ”the Examiner reads the claimed "sequential code" upon Barnett's character string (See Page 8 of the 6/25/2008 Office Action). However, as noted above. Bamett 's character string is not including in the data packet transmission Rather, only tile encrypted data and tile transport key are included in the data packet. Accordingly, even if one were to accept the Examiner's interpretation that the claim limitation "said first unique code being derived from a first sequential code" reads on Barnett such that tile "first unique code" corresponds to the unique encryption key, and the "first sequential code" corresponds to the character string, Barnett under this interpretation clearly could not disclose or suggest "encapsulating said first encrypted data frame in a First transport frame, said t%~1 transport frame comprising first portion a and (a second portion of said first sequential code " (Emphasis added) as recited in

independent claim 1 and similarly recited in independent claims 4, 7, 10, 13, 17, 21 and 25 because the character string in 13 Barnett is not included in the same. "Also, if the Examiner were to change the above- noted interpretation to read the "sequential code:' on the transport key, Applicant notes that the transport key is not used to derive the unique encryption key; rather, the character string is used to derive both keys (e.g., .See .Barnett at Col. 3, lines 44-56). The examiner, respectfully disagrees and submits that Barnett et all was use to show that a unique encryption code is generated based on sequential code (See column 2, lines 25-31; column 3, lines 49-59 and column 6, lines 14-17). Therefore the examiner submits that the combine teaching of Alden et al, Citta et al and Barnett discloses the claimed invention see the below argument.

Applicant admits that Alden discloses “(i) receiv[ing] a message or packet, (ii) encrypt[ing] the packet, (iii) encapsulat[ingj the encrypted packer with a data frame for transmission, and (iv) transmit[ting] the data frame to another device.” See response at page 12. Emphasis added.

However, Applicant contends that, “the pseudo network of Alden can only apply the same encryption to all packets” Accordingly, according to Applicant, Alden fails to teach “encrypting a first data frame based on a first unique code” and “encrypting a second data frame based on a second unique code.”

Citta discloses such limitation. Citta discloses applying different encryption to different data packets, as recognized by Applicant.

Applicant notes that Alden fails to disclose “sequential code encryption”. However, Citta was used for this limitation, as also acknowledged by Applicant.

5. Applicant admits that, “Citta does disclose applying different encryption to different data packets”. See response at page 15. Emphasis added.

6. However, Applicant asserts that, “both Alden and Citta fail to disclose or suggest deriving a unique encryption code based on a sequential code, using the unique encryption code to encrypt a data frame and then encapsulating the sequential code with the data frame.” Emphasis added.

First, it should be noted, it is “encrypted data frame” that is encapsulated into a transport frame, not the “sequential code” as argued by Applicant.

In summary, Applicant argues that none of the applied prior art references teaches “deriving a unique encryption code based on a sequential code, using the unique encryption code to encrypt a data frame.”

As explained above, Alden discloses “(i) receiving a message/packet, (ii) encrypting the packet, (iii) encapsulating the encrypted packer with a data frame for transmission, and (iv) transmitting the data frame to another device.

Also, Citta does disclose applying different encryption to different data packets.

However, neither Alden nor Citta particularly discloses a using a sequential code for which a unique key is derived for encrypting the data.

It should be noted that the specification does not clearly define “sequential code”. It merely discloses a sequential code in connection the data encryption. Therefore, giving the limitation “sequential code” its broadest interpretation (MPEP 2111), the following references are used for the teaching of “sequential code”.

Penman (6,363,480) discloses a plurality of keys for encrypting a message (abstract). Figure 2 of Perlman shows a set of keys ({KEY}(32) to be used to encrypt {MESSAGE}(34).. See also Fig 4; column 31 line 66 to column 4, line 2.

Bamett (6,661,896) discloses a computer network security system and method, wherein there is provided a unique key program (42) for generating a unique key based on a character phrase (46). The generated unique key is used to encrypt a data packet (52) and the encrypted data packet is transmitted (54) to another device. The character phrase corresponds to the claimed “sequential code” as the unique key is generated based on the character phrase. See column 2, lines 25-31; column 3, lines 49-59 and column 6, lines 14-17.

Kluttz et al (6,598,161) discloses methods, systems and computer program products for multi-level encryption, wherein different encryption keys are used to encrypt different data packets (documents). See abstract. According to Kluttz et al, the document is sequentially encrypted utilizing at least two encryption keys (abstract). As shown in figure 2, there is provided a set of encryption keys (72) from which a plurality of keys (104, 106, 108) are drawn in order to encrypt the document. The different levels of the document (200) correspond to the claimed first and second data frame. See figures 4 and 5, column 2, lines 15-20; column 9, lines 10-17.

With respect to the other references, Applicant merely states these references “fail[sl to cure the suggestion and disclosure deficiencies of Alden in view of Citta related to independent claims 1, 4, 7, 10.”

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a. A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1, 4, 7, 10, 13-28, 33 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alden et al (US 6,101,543) in view of Citta et al (US 4,771,458) in further view of Barnett (US 6,661,896).

Claims 1, 4, 7 and 10: Alden et al discloses a method, a computer readable medium, and an apparatus for transmitting packet from a local communications protocol stack to a virtual private network comprising:

i. A receiver (Fig.14, item 253);

ii. A transmitter (Fig.14); and

iii. A processor communicatively coupled to the-receiver and the transmitter, the processor being capable of implementing a method for synchronizing encryption and decryption of a data frame in a communication network (column 14, lines 11-37);

iv. Encrypting a first data frame based on a first unique code in a first communication device, said first unique code being derived from a first sequential code (the transmit path includes an encryption engine for encrypting the data packet) (column 3, lines 18-19), but does explicitly disclose that a sequential encryption is used.

v. Encapsulating said first encrypted data frame in a first transport frame, said first transport frame comprising a first portion and a second portion of said first sequential code (and encapsulation engine for encapsulating the encrypted data packets into tunnel data frames) (column 3, lines 19-21);

vi. Encrypting a second data frame based on a second unique code in the first communication device, said second unique code being derived from a second sequential code the transmit path includes an encryption engine for encrypting the data packet) (column 3, lines 18-19), but does explicitly disclose that a sequential encryption is used.

vii. Encapsulating said second encrypted data frame in a second transport frame, said second transport frame comprising a first portion and a second portion of said second sequential code (and encapsulation engine for encapsulating the encrypted data packets into tunnel data frames) (column 3, lines 19-21);

viii. And transmitting said first transport frame and said second transport frame to a second communication device, wherein said first portion of said first sequential code and said first portion of said second sequential code identify the same relative portions of said first and second sequential codes, and said second portion of said second sequential code represents a successive relative portion with respect to said second portion of said first sequential code (the new pseudo network adapter

includes a transmit path for processing data packets from the local communications protocol stack for transmission through the pseudo network adapter) (column 3 , lines 15-19).

Alden et al does not disclose that the encryption is based on sequential code encryption. However Citta et al discloses a secure data packet transmission, which used a sequential encryption (DEEP feature, as will be seen, simultaneously encrypts and error protects the data) (column1, lines 60-65; column 2, lines 54-65; column 3, lines 10-15). While neither of them explicitly discloses a step of deriving a unique encryption code based on sequential code. However, Barnett discloses a computer network security , which further discloses a step of deriving a unique encryption code based on sequential code(wherein there is provided a unique key program (42) for generating a unique key based on a character phrase (46). The generated unique key is used to encrypt a data packet (52) and the encrypted data packet is transmitted (54) to another device. The character phrase corresponds to the claimed “sequential code” as the unique key is generated based on the character phrase. See column 2, lines 25-31; column 3, lines 49-59 and column 6, lines 14-17). Therefore, it would have been obvious for one having ordinary skills in the art at the time the invention was made to modify the combined teaching of Alden et al and Citta et al such as to use an encryption based on sequential keys. One would have been motivate to do so in order to provide a secure, readily implemented data packet transmission system as taught by Citta et al (column 3, lines 2-6).

Claims 13, 17, 21 and 25: Alden et al discloses a method, a computer readable medium, and an apparatus for transmitting packet from a local communications protocol stack to a virtual private network comprising:

i. A receiver (Fig.14, item 253);

ii. A transmitter (Fig.14); and

iii. A processor communicatively coupled to the-receiver and the transmitter, the processor being capable of implementing a method for synchronizing encryption and decryption of a data frame in a communication network (column 14, lines 11-37);

iv. Receiving a first transport frame, said first transport frame comprising a first encrypted data payload, a first portion of a first sequential code, and a second portion of said first sequential code (the new network adapter further include an interface into a transport layer of the local communication protocol stack for capturing received data packets from the remote server node and a receive path for processing received data packet) (column 3, lines 40-45);

v. Receiving a second transport frame, said second transport frame comprising a second encrypted data payload, a first portion of a second sequential code, and a second portion of said second sequential code (the new network adapter further include an interface into a transport layer of the local communication protocol stack for capturing received data

packets from the remote server node and a receive path for processing received data packet) (column 3, lines 40-45);

vi. And determining said second sequential code using said first portion of said second sequential code, said second portion of said second sequential code, and said second portion of said first sequential code, wherein said first portion of said first sequential code and said first portion of said second sequential code identify the same relative portions of said first and second sequential codes, and said second portion of said second sequential code represents a successive relative portion with respect to said second portion of said first sequential code (the new pseudo network adapter includes a transmit path for processing data packets from the local communications protocol stack for transmission through the pseudo network adapter) (column 3 , lines 15-19).

Alden et al does not disclose that the encryption is based on sequential code encryption. However Citta et al discloses a secure data packet transmission, which used a sequential encryption (DEEP feature, as will be seen, simultaneously encrypts and error protects the data) (column1, lines 60-65; column 2, lines 54-65; column 3, lines 10-15). While neither of them explicitly discloses a step of deriving a unique encryption code based on sequential code. However, Barnett discloses a computer network security , which further discloses a step of deriving a unique encryption code based on sequential code(wherein there is provided a unique key program (42) for generating a unique key based

on a character phrase (46). The generated unique key is used to encrypt a data packet (52) and the encrypted data packet is transmitted (54) to another device. The character phrase corresponds to the claimed "sequential code" as the unique key is generated based on the character phrase. See column 2, lines 25-31; column 3, lines 49-59 and column 6, lines 14-17). Therefore, it would have been obvious for one having ordinary skills in the art to modify the combined teaching of Alden et al and Citta et al such as to use an encryption based on sequential keys. One would have been motivate to do so in order to provide a secure, readily implemented data packet transmission system as taught by Citta et al (column 3, lines 2-6).

Claims 14, 18, 22 and 26: Alden et al , Citta et al and Barnett disclose a method, system and apparatus for transmitting packet from a local communications protocol stack to a virtual private network as in claims 13, 17, 21 and 25above, and Citta et al further discloses that decrypting of said second encrypted data payload using said second sequential code (the invention resides in the intertwining of the address decryption key) (column 7, lines 15-35). Therefore, it would have been obvious for one having ordinary skills in the art at the time the invention was made to modify the combined teaching of Alden et al and Barnett such as to use a decryption based on sequential keys. One would have been motivate to do so in order to increase data integrity.

Claims 15, 19, 23 and 27: Alden et al , Citta et al and Barnett disclose a method, a computer readable medium, and an apparatus for transmitting packet

from a local communications protocol stack to a virtual private network as in claims 13, 17, 21 and 25 above, and Citta et al further discloses that determining said first sequential code using said first portion of said first sequential code, said second portion of said first sequential code, and said second portion of said second sequential code (The bit packets are assembled with a global bit packet encrypted with a global encryption key and subsequent individually addressed bit packets encrypted with address keys) (column 4, line 43 to column 5 line 15; abstract). Therefore, it would have been obvious for one having ordinary skills in the art at the time of the invention to modify the combined teaching of Alden et al and Barnett such as to distinguish between different portions of the encryption code. One would have been motivate to do so in order to increase data integrity.

Claims 16, 20, 24 and 28: Alden et al , Citta et al and Barnett disclose a method, a computer readable medium, and an apparatus for transmitting packet from a local communications protocol stack to a virtual private network as in claims 15, 19, 23 and 27 above, and Citta et al further discloses that decrypting of said first encrypted data payload using said first sequential code (A number of global decryption keys which are cycled through in attempts to decrypt the global packets are stored in each subscriber terminal) (column 5, lines 4-15). Therefore, it would have been obvious for one having ordinary skills in the art at the time of the invention to modify the combined teaching of Alden et al and Barnett such as to use a decryption based on sequential keys. One would have been motivate to do so in order to increase data integrity.

Claim 33: Alden et al , Citta et al and Barnett disclose a method, a computer readable medium, and an apparatus for transmitting packet from a local communications protocol stack to a virtual private network as in claim 1 above, and Alden et al further discloses wherein the encrypting and encapsulating steps are performed at a transport layer Of an Open System Interconnection (OSI) standard (Now with reference to FIG. 1 there is described for purposes of explanation, communications based on the Open Systems Interconnection (OSI) reference model)(column 4, line65 to column 5 line15).

Claim 34: Alden et al , Citta et al and Barnett disclose a method, a computer readable medium, and an apparatus for transmitting packet from a local communications protocol stack to a virtual private network as in claim 1 above, and Alden et al further discloses wherein the encrypting of the first and second data frames is not based on a level of encryption associated with a higher-layer data object that includes data present within one of the first and second data frames (Fig.21 and Fig. 22).

9. Claims 2, 5, 8, 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alden et al (US 6101543) in view of Citta et al (US 4,771,458) and Barnett (US 6,661,896) in further view of Perlman (US 6363480).

Claims 2, 5, 8, 11: Alden et al, Citta et al and Barnett disclose a method, an apparatus, and a computer readable medium for transmitting packet from a local communications protocol stack to a virtual private network as in claims 1, 4, 7,

and 10 above, but do not explicitly disclose that said first portion of said first sequential code and said first portion of said second sequential code each represent a short-term component of said first and second sequential codes. However, Perlman discloses a system and method for a user to encrypt data in a way that ensures data cannot be decrypted after a finite period, which further short-term component of said first and second sequential codes (provide one or more ephemeral encryption keys to party wishing to encrypt a message to be passed to a destination party (column 2, lines 45-53). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method, apparatus, and computer readable medium of Alden et al , Citta et al and Barnett such as to use ephemeral keys in the encryption process. The motivation for doing so would have been to protect against attempts to retrieve critical information.

10. Claims 3, 6, 9, 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alden et al (US 6101543) in view of Citta et al (US 4,771,458) and Barnett (US 6,661,896). in further view of Semper (US 6657984).

Claims 3, 6, 9, and 12: Alden et al, Citta et al and Barnett disclose a method, an apparatus, and a computer readable medium for transmitting packet from a local communications protocol stack to a virtual private network as in claims 1, 4, 7, and 10 above, but do not explicitly disclose the transport frame comprises a radio link protocol (RLP) frame. However, Semper discloses a system, method, and

apparatus for providing backward compatibility of radio link protocols in a wireless network, which further discloses a transport frame, comprises a radio link protocol (the system comprises a radio link protocol) (column 2, lines 10-15 Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined teaching of Alden et al , Citta et al and Barnett such as to use a radio link protocol. One would have been motivate to do so in order to reduce packets loss rate during transmission.

11. Claims 1, 4, 7, 10, 13-28, 33 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alden et al (US 6,101,543) in view of Citta et al (US 4,771,458) in further view of Kluttz et al(US 6,598,161).

Claims 1, 4, 7 and 10: Alden et al discloses a method, a computer readable medium, and an apparatus for transmitting packet from a local communications protocol stack to a virtual private network comprising:

i. A receiver (Fig.14, item 253);

ii. A transmitter (Fig.14); and

iii. A processor communicatively coupled to the-receiver and the transmitter, the processor being capable of implementing a method for synchronizing encryption and decryption of a data frame in a communication network (column 14, lines 11-37);

iv. Encrypting a first data frame based on a first unique code in a first communication device, said first unique code being derived from a first sequential code (the transmit path includes an encryption engine for

encrypting the data packet) (column 3, lines 18-19), but does explicitly disclose that a sequential encryption is used.

v. Encapsulating said first encrypted data frame in a first transport frame, said first transport frame comprising a first portion and a second portion of said first sequential code (and encapsulation engine for encapsulating the encrypted data packets into tunnel data frames) (column 3, lines 19-21);

vi. Encrypting a second data frame based on a second unique code in the first communication device, said second unique code being derived from a second sequential code the transmit path includes an encryption engine for encrypting the data packet) (column 3, lines 18-19), but does explicitly disclose that a sequential encryption is used.

vii. Encapsulating said second encrypted data frame in a second transport frame, said second transport frame comprising a first portion and a second portion of said second sequential code (and encapsulation engine for encapsulating the encrypted data packets into tunnel data frames) (column 3, lines 19-21);

viii. And transmitting said first transport frame and said second transport frame to a second communication device, wherein said first portion of said first sequential code and said first portion of said second sequential code identify the same relative portions of said first and second sequential codes, and said second portion of said second sequential code

represents a successive relative portion with respect to said second portion of said first sequential code (the new pseudo network adapter includes a transmit path for processing data packets from the local communications protocol stack for transmission through the pseudo network adapter) (column 3 , lines 15-19).

Alden et al does not disclose that the encryption is based on sequential code encryption. However Citta et al discloses a secure data packet transmission, which used a sequential encryption (DEEP feature, as will be seen, simultaneously encrypts and error protects the data) (column1, lines 60-65; column 2, lines 54-65; column 3, lines 10-15). While neither of them explicitly discloses a step of deriving a unique encryption code based on sequential code. However, Kluttz et al discloses a program product for multi- level encryption , which further discloses a step of deriving a unique encryption code based on sequential code(, the document is sequentially encrypted utilizing at least two encryption keys (abstract). As shown in figure 2, there is provided a set of encryption keys (72) from which a plurality of keys (104, 106, 108) are drawn in order to encrypt the document. The different levels of the document (200) correspond to the claimed first and second data frame. See figures 4 and 5, column 2, lines 15-20; column 9, lines 10-17). Therefore, it would have been obvious for one having ordinary skills in the art at the time the invention was made to modify the combined teaching of Alden et al and Citta et al such as to use an encryption based on sequential keys. One would have been motivate to

do so in order to provide a secure, readily implemented data packet transmission system as taught by Citta et al (column 3, lines 2-6).

Claims 13, 17, 21 and 25: Alden et al discloses a method, a computer readable medium, and an apparatus for transmitting packet from a local communications protocol stack to a virtual private network comprising:

i. A receiver (Fig.14, item 253);

ii. A transmitter (Fig.14); and

iii. A processor communicatively coupled to the-receiver and the transmitter, the processor being capable of implementing a method for synchronizing encryption and decryption of a data frame in a communication network (column 14, lines 11-37);

iv. Receiving a first transport frame, said first transport frame comprising a first encrypted data payload, a first portion of a first sequential code, and a second portion of said first sequential code (the new network adapter further include an interface into a transport layer of the local communication protocol stack for capturing received data packets from the remote server node and a receive path for processing received data packet) (column 3, lines 40-45);

v. Receiving a second transport frame, said second transport frame comprising a second encrypted data payload, a first portion of a second sequential code, and a second portion of said second sequential code (the new network adapter further include an interface into a transport layer of

the local communication protocol stack for capturing received data packets from the remote server node and a receive path for processing received data packet) (column 3, lines 40-45);

vi. And determining said second sequential code using said first portion of said second sequential code, said second portion of said second sequential code, and said second portion of said first sequential code, wherein said first portion of said first sequential code and said first portion of said second sequential code identify the same relative portions of said first and second sequential codes, and said second portion of said second sequential code represents a successive relative portion with respect to said second portion of said first sequential code (the new pseudo network adapter includes a transmit path for processing data packets from the local communications protocol stack for transmission through the pseudo network adapter) (column 3 , lines 15-19).

Alden et al does not disclose that the encryption is based on sequential code encryption. However Citta et al discloses a secure data packet transmission, which used a sequential encryption (DEEP feature, as will be seen, simultaneously encrypts and error protects the data) (column1, lines 60-65; column 2, lines 54-65; column 3, lines 10-15). While neither of them explicitly discloses a step of deriving a unique encryption code based on sequential code. However, Kluttz discloses a method, system, and computer program product for multi level encryption, which further discloses a step of deriving a unique

encryption code based on sequential code(, the document is sequentially encrypted utilizing at least two encryption keys (abstract). As shown in figure 2, there is provided a set of encryption keys (72) from which a plurality of keys (104, 106, 108) are drawn in order to encrypt the document. The different levels of the document (200) correspond to the claimed first and second data frame. See figures 4 and 5, column 2, lines 15-20; column 9, lines 10-17.). Therefore, it would have been obvious for one having ordinary skills in the art to modify the combined teaching of Alden et al and Citta et al such as to use an encryption based on sequential keys. One would have been motivate to do so in order to provide a secure, readily implemented data packet transmission system as taught by Citta et al (column 3, lines 2-6).

Claims 14, 18, 22 and 26: Alden et al , Citta et al and Kluttz et al disclose a method, system and apparatus for transmitting packet from a local communications protocol stack to a virtual private network as in claims 13, 17, 21 and 25above, and Citta et al further discloses that decrypting of said second encrypted data payload using said second sequential code (the invention resides in the intertwining of the address decryption key) (column 7, lines 15-35). Therefore, it would have been obvious for one having ordinary skills in the art at the time the invention was made to modify the combined teaching of Alden et al and Kluttz et al such as to use a decryption based on sequential keys. One would have been motivate to do so in order to increase data integrity.

Claims 15, 19, 23 and 27: Alden et al , Citta et al and Kluttz et al disclose a method, a computer readable medium, and an apparatus for transmitting packet from a local communications protocol stack to a virtual private network as in claims 13, 17, 21 and 25 above, and Citta et al further discloses that determining said first sequential code using said first portion of said first sequential code, said second portion of said first sequential code, and said second portion of said second sequential code (The bit packets are assembled with a global bit packet encrypted with a global encryption key and subsequent individually addressed bit packets encrypted with address keys) (column 4, line 43 to column 5 line 15; abstract). Therefore, it would have been obvious for one having ordinary skills in the art at the time of the invention to modify the combined teaching of Alden et al and Kluttz et al such as to distinguish between different portions of the encryption code. One would have been motivate to do so in order to increase data integrity.

Claims 16, 20, 24 and 28: Alden et al , Citta et al and Kluttz et al disclose a method, a computer readable medium, and an apparatus for transmitting packet from a local communications protocol stack to a virtual private network as in claims 15, 19, 23 and 27 above, and Citta et al further discloses that decrypting of said first encrypted data payload using said first sequential code (A number of global decryption keys which are cycled through in attempts to decrypt the global packets are stored in each subscriber terminal) (column 5, lines 4-15). Therefore, it would have been obvious for one having ordinary skills in the art at the time of the invention to modify the combined teaching of Alden et al and Kluttz et al such

as to use a decryption based on sequential keys. One would have been motivate to do so in order to increase data integrity.

Claim 33: Alden et al , Citta et al and Barnett disclose a method, a computer readable medium, and an apparatus for transmitting packet from a local communications protocol stack to a virtual private network as in claim 1 above, and Alden et al further discloses wherein the encrypting and encapsulating steps are performed at a transport layer Of an Open System Interconnection (OSI) standard (Now with reference to FIG. 1 there is described for purposes of explanation, communications based on the Open Systems Interconnection (OSI) reference model)(column 4, line65 to column 5 line15).

Claim 34: Alden et al , Citta et al and Barnett disclose a method, a computer readable medium, and an apparatus for transmitting packet from a local communications protocol stack to a virtual private network as in claim 1 above, and Alden et al further discloses wherein the encrypting of the first and second data frames is not based on a level of encryption associated with a higher-layer data object that includes data present within one of the first and second data frames (Fig.21 and Fig. 22).

12. Claims 2, 5, 8, 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alden et al (US 6101543) in view of Citta et al (US 4,771,458) and Kluttz et al(US 6,598,161) in further view of Perlman (US 6363480).

Claims 2, 5, 8, 11: Alden et al, Citta et al and Kluttz et al disclose a method, an apparatus, and a computer readable medium for transmitting packet from a local communications protocol stack to a virtual private network as in claims 1, 4, 7, and 10 above, but do not explicitly disclose that said first portion of said first sequential code and said first portion of said second sequential code each represent a short-term component of said first and second sequential codes. However, Perlman discloses a system and method for a user to encrypt data in a way that ensures data cannot be decrypted after a finite period, which further short-term component of said first and second sequential codes (provide one or more ephemeral encryption keys to party wishing to encrypt a message to be passed to a destination party (column 2, lines 45-53). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method, apparatus, and computer readable medium of Alden et al , Citta et al and Kluttz et al such as to use ephemeral keys in the encryption process. The motivation for doing so would have been to protect against attempts to retrieve critical information.

13. Claims 3, 6, 9, 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alden et al (US 6101543) in view of Citta et al (US 4,771,458) and Kluttz et al(US 6,598,161) in further view of Semper (US 6657984).

Claims 3, 6, 9, and 12: Alden et al, Citta et al and Kluttz et al disclose a method, an apparatus, and a computer readable medium for transmitting packet from a

local communications protocol stack to a virtual private network as in claims 1, 4, 7, and 10 above, but do not explicitly disclose the transport frame comprises a radio link protocol (RLP) frame. However, Semper discloses a system, method, and apparatus for providing backward compatibility of radio link protocols in a wireless network, which further discloses a transport frame, comprises a radio link protocol (the system comprises a radio link protocol) (column 2, lines 10-15 Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined teaching of Alden et al , Citta et al and Kluttz et al such as to use a radio link protocol. One would have been motivate to do so in order to reduce packets loss rate during transmission.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

2. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT,

Monday, December 08, 2008

/Carl Colin/

Primary Examiner, Art Unit 2436